(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023717 A2

(51) International Patent Classification⁷: H04L 9/32, 9/28, H04N 7/167, H04K 1/00

(21) International Application Number: PCT/US2003/027774

(22) International Filing Date: 8 September 2003 (08.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/409,675 9 September 2002 (09.09.2002) US

(71) Applicant: SONY ELECTRONICS INC. [US/US]; 1 Sony Drive, Park Ridge, NJ 07656 (US).

(72) Inventor: CANDELORE, Brant, L.; 10124 Quail Glen Way, Escondido, CA 92029-6502 (US).

(74) Agents: KANANEN, Ronald, P. et al.; RADER FISHMAN & GRAUER PLLC, 1233 20th Street, NW, Suite 501, Washington, DC 20036 (US).

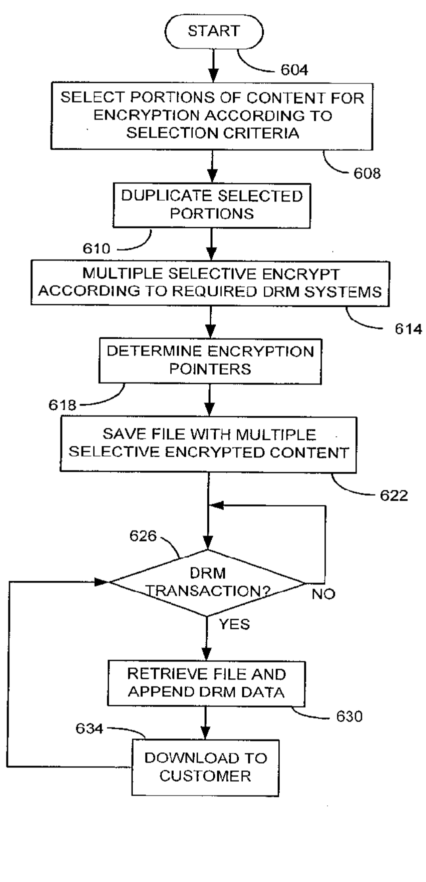
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: CONTENT DISTRIBUTION FOR MULTIPLE DIGITAL RIGHTS MANAGEMENT

600



(57) Abstract: A method and apparatus for enabling use of multiple digital rights management scenarios (DRM). Unencrypted data representing digital content is examined to identify at least segments of content for encryption. The identified segments of content are duplicated and then encrypted using a first encryption method associated with a first DRM to produce first encrypted segments. Duplicates are encrypted using a second encryption method associated with a second DRM to produce second encrypted segments. A set of pointers are generated that point to the first and second encrypted segments content. A file is then created containing first and second encrypted segments of content, pointers and unencrypted content along with DRM rights data to produce a selectively encrypted multiple DRM enabled file.

WO 2004/023717 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

CONTENT DISTRIBUTION FOR MULTIPLE DIGITAL RIGHTS MANAGEMENT

CROSS REFERENCE TO RELATED DOCUMENTS

This application is related to U.S. patent applications serial number 10/273,905, filed October 18, 2002 to Candelore et al. entitled "Video Slice and Active Region Based Dual Partial Encryption", serial number 10/273,903, filed October 18, 2002 to Candelore et al. entitled "Star Pattern Partial Encryption", serial number 10/274,084, filed October 18, 2002 to Candelore et al. entitled "Slice Mask and Moat Pattern Partial Encryption", and serial number 10/274,019, filed October 18, 2002 to Candelore et al. entitled "Video Scene Change Detection", which are hereby incorporated by reference.

This application is also related to and claims priority benefit of U.S. Provisional patent application serial number 60/409,675, filed September 9, 2002, entitled "Generic PID Remapping for Content Replacement", to Candelore. This application is also hereby incorporated by reference herein.

COPYRIGHT NOTICE

FIELD OF THE INVENTION

This invention relates generally to the field of digital rights management. More particularly, this invention relates to a multiple encryption method and apparatus particularly useful for multiple encrypting digitized video for purposes of enabling multiple digital rights management scenarios (DRMs).

BACKGROUND OF THE INVENTION

In traditional distribution of audio and/or video content such as music and movies, rights to copyrighted works are managed by the ownership of the physical medium containing the work. Ownership of the medium provides a limited barrier to unauthorized use. While piracy was and is prevalent with such traditional "packaged media", the problems are dramatically multiplied in an environment of digital distribution of content. The owners of the content have devised various ways to help protect such content that have been collectively termed digital rights management (DRM). DRM encompasses not only the numerous encryption schemes that have been employed to protect the content, but also encompasses the various arrangements for permitting use of the content that have been created, as well as the monitoring and tracking of the rights to the content.

Several forms of DRM are currently in place in the marketplace. Perhaps the most dominant DRM forms a part of the Microsoft Windows® operating system's Media Player, and is referred to as "Reciprocal". Another widely used

DRM arrangement is built into the Real Networks' Real Player®. Currently the DRM solutions from Microsoft is tightly coupled with the compression algorithm. DRM solutions usually execute on personal computer (PC) platforms. Consequently, the DRM solutions are designed to detect software tampering, and thus efforts are made to obfuscate the operation of the executing software.

The above two examples of DRM are but two of an ever growing and evolving field of technology. Further DRM incarnations can be anticipated on a continuing basis to provide greater protection for the content against those who would illegally pirate the content.

Unfortunately, due to the multiple types of DRM that are available, customers may have to either acquire multiple sets of software (or plug-ins) that support the various DRM scenarios, or limit consumption of content to those DRMs which they wish to support on their computer.

BRIEF DESCRIPTION OF THE DRAWINGS

The features of the invention believed to be novel are set forth with particularity in the appended claims. The invention itself however, both as to organization and method of operation, together with objects and advantages thereof, may be best understood by reference to the following detailed description of the invention, which describes certain exemplary embodiments of the invention, taken in conjunction with the accompanying drawings in which:

FIGURE 1 is a block diagram of an digital content distribution system including digital rights management consistent with certain embodiments of the present invention.

FIGURE 2 illustrates an exemplary file structure consistent with certain embodiments of the present invention.

FIGURE 3 illustrates a byte offset arrangement for video data consistent with certain embodiments of the present invention.

FIGURE 4 illustrates a byte offset arrangement for audio data consistent with certain embodiments of the present invention.

FIGURE 5 illustrates an exemplary DRM arrangement within video or audio data content consistent with certain embodiments of the present invention.

FIGURE 6 is a flow chart showing a method for encoding content with multiple DRMs consistent with certain embodiments of the present invention.

FIGURE 7 is a flow chart depicting acquisition and playback of content having multiple DRMs consistent with certain embodiments of the present invention.

FIGURE 8 illustrates a content provider server system consistent with certain embodiments of the present invention.

FIGURE 9 is a block diagram of a playback computer consistent with embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

While this invention is susceptible of embodiment in many different forms, there is shown in the drawings and will herein be described in detail specific embodiments, with the understanding that the present disclosure is to be considered as an example of the principles of the invention and not intended to limit the invention to the specific embodiments shown and described. In the description below, like reference numerals are used to describe the same, similar or corresponding parts in the several views of the drawings.

The terms "scramble" and "encrypt" and variations thereof are used synonymously herein. The term "video" is often used herein to embrace not only true visual information, but also in the conversational sense (e.g., "video tape recorder") to embrace not only video signals but associated audio and data. The present document generally uses the example of a "dual selective encryption" embodiment, but those skilled in the art will recognize that the present invention can be utilized to realize multiple partial encryption without departing from the

invention. The terms "partial encryption" and "selective encryption" are used synonymously herein.

The above-referenced commonly owned patent applications describe inventions relating to various aspects of methods generally referred to herein as partial encryption or selective encryption. More particularly, systems are described wherein selected portions of a particular selection of digital content are encrypted using two (or more) encryption techniques while other portions of the content are left unencrypted. By properly selecting the portions to be encrypted, the content can effectively be encrypted for use under multiple decryption systems without the necessity of encryption of the entire selection of content. In some embodiments, only a few percent of data overhead is needed to effectively encrypt the content using multiple encryption systems. This results in a cable or satellite system being able to utilize Set-top boxes or other implementations of conditional access (CA) receivers from multiple manufacturers in a single system - thus freeing the cable or satellite company to competitively shop for providers of Set-top boxes.

The present invention applies similar selective encryption techniques to the problem of multiple digital rights management. The partial encryption processes described in the above patent applications utilize any suitable encryption method. However, these encryption techniques are selectively applied to the data stream, rather than encrypting the entire data stream, using techniques described in the above-referenced patent applications. In general, but without the intent to be limiting, the selective encryption process utilizes intelligent selection of information to encrypt so that the entire program does not have to undergo dual encryption. By appropriate selection of data to encrypt, the program material can be effectively scrambled and hidden from those who desire to hack into the system and illegally recover commercial content without paying. MPEG (or similar format) data that are used to represent the audio and video data does so using a high degree of reliance on the redundancy of information

from frame to frame. Certain data can be transmitted as "anchor" data representing chrominance and luminance data. That data is then often simply moved about the screen to generate subsequent frames by sending motion vectors that describe the movement of the block. Changes in the chrominance and luminance data are also encoded as changes rather than a recoding of absolute anchor data. Thus, encryption of this anchor data, for example, or other key data can effectively render the video un-viewable.

Certain embodiments of the present invention enable a second (or multiple) Digital Rights Management (DRM) solution by duplicating and encrypting content important or critical for decoding the rest of the content with the first and second DRMs. The duplication of content need not add a major increase bandwidth overhead. Unlike terrestrial and satellite broadcast streams, content delivered and eventually decrypted by a PC over the internet does not have to be restricted to 188 byte packets. For terrestrial and satellite streams, hardware decryption is usually performed on per packet basis based on the scrambling bits in the transport header. Content decryption done in software can be much more granular and selective.

In accordance with certain embodiments consistent with the present invention, the selected video data to be encrypted may be any individual one or combination of the following (described in greater detail in the above applications): video slice headers appearing in an active region of a video frame, data representing an active region of a video frame, data in a star pattern within the video frame, data representing scene changes, I Frame packets, packets containing motion vectors in a first P frame following an I Frame, packets having an intra_slice_flag indicator set, packets having an intra_slice indicator set, packets containing an intra_coded macroblock, data for a slice containing an intra_coded macroblock, data from a first macroblock following the video slice header,packets containing video slice headers, anchor data, and P Frame data for progressively refreshed video data, data arranged in vertical and or horizontal

moat patterns on the video frame, and any other selected data that renders the video and/or audio difficult to utilize. Several such techniques as well as others are disclosed in the above-referenced patent applications, any of which (or other techniques) can be utilized with the present invention to encrypt only a portion of the content.

Referring now to **FIGURE 1**, a content delivery system 100 consistent with certain embodiments of the present invention is illustrated. In this system, a digital content provider 104 provides content such as audio or video content to a customer over the Internet for delivery to the customer's personal computer system 112, e.g., by downloading or streaming. Computer system 112 may, for example, be a multimedia computer system having a video display 116 and a stereo (or other multi-channel) audio system that drives a set of speakers such as speakers 120L and 120R. The personal computer 112 operates using any suitable operating system and incorporates one or more software programs for playback of the audio and/or video content (hereinafter, a "media player").

The digital content provider may operate as an addressable web site that serves as an online distributor of content. In this example, the web site is shown to have a content database 130 that stores content which can be purchased under various terms by customers having computers such as 112 connected to the Internet. To provide a simplified example, without intent to limit the scope of the present invention, digital content provider 104 is depicted as having the ability to supply content using two digital rights management systems - DRM A shown as 134 and DRM B shown as 138. In a conventional digital content provider scenario, only a single DRM system is used and content is stored in encrypted form using the encryption scenario for that particular DRM system.

In accordance with certain embodiments consistent with the present invention, content stored in the content database 130 is stored with dual (in general multiple) selective encryption consistent with the content provider's dual (multiple) DRMs. In this manner, the digital content provider 104 is not burdened

with the requirement and cost associated with storage of the content separately under multiple DRMs. Nor is the computing power required to dynamically encrypt the content using a specified DRM at the time of purchase.

Content can be arranged for delivery to the customer as a file similar to that depicted in **FIGURE 2**. In this file structure, the file delivered to the customer is stored with selected portions multiply encrypted. In one example, not intended to be limiting, if the content is stored as MPEG data, one can encrypt all of the MPEG I frames or video slice headers to achieve a substantial level of encryption without need to encrypt the entire file. Any other suitable selective encryption arrangement can also be used without limitation. Once a selected portion of the audio and/or video is selected for encryption, the selected portions are duplicated and encrypted. In this example, the selected portions are encrypted under an encryption arrangement consistent with DRM A in one case and consistent with DRM B in the other. The content is then reassembled with the duplicated encrypted content replacing the original clear content. (Note that in other scenarios, content can be stored encrypted or unencrypted and the file processed and constructed for delivery to the customer "on the fly".)

In this example of Audio/Video content, the content is stored as audio content 206 and video content 210. The file further contains a set of audio encryption pointers 212 that point to the selected portions of the audio content that are encrypted. Similarly, the file further contains a set of video encryption pointers 218 that point to the selected portions of the video content that are encrypted. DRM A data section 222 provides data that the decoder will need to decode the content encrypted using the encryption scheme of DRM A. Similarly, DRM B data section 226 provides data that the decoder will need to decode the content encrypted using the encryption scheme of DRM B. An identification section 230 identifies the content and the DRM schemes available in the file.

The relationship between the video data 210 and video encryption pointers 218 is illustrated in **FIGURE 3**. Pointers are stored that point to

encrypted portions of the video data in the file. Such encrypted portions are shown as 304, 308 and 312. Such encrypted portions are interspersed with portions of data stored unencrypted (In the clear) shown as 320, 324, 328 and 332. Of course this illustration is quite simplified since only a small number of encrypted segments are shown compared to the likely large number of encrypted segments. In this illustration, each encrypted segment is illustrated to be the same size (i.e., the encryption quanta), but this is not to be interpreted as limiting.

The relationship between the audio data 206 and audio encryption pointers 212 is similar and illustrated in **FIGURE 4**. Pointers are stored that point to encrypted portions of the audio data in the file. Such encrypted portions are shown as 404, 408 and 412. Such encrypted portions are interspersed with portions of data stored unencrypted shown as 420, 424, 428 and 432. Again, this illustration is quite simplified since only a small number of encrypted segments are shown compared to the likely large number of encrypted segments. In this illustration, the encrypted segments are shown as differing in size, which can be achieved by specifying the length of each encrypted segment.

In each case, the number of bytes to be encrypted can be predefined if desired as the encryption quanta so that the encryption pointers can be simply a sequence of memory offset locations. The amount of data encrypted is then determined by a preset encryption quanta (e.g., 8 bytes). In other embodiments, the encryption pointer section can include not only a starting offset but also an ending offset or a starting offset and a number of bytes.

FIGURE 5 depicts an exemplary section of encrypted content with the byte offset location illustrated at the beginning of the section of encrypted content. The next segment of data is DRM A encrypted content 502 that lasts for a duration determined by the encryption quanta (either predefined or encoded in the encryption pointers). The next segment of encrypted content 506 is encrypted under DMA B's encryption scheme and lasts for a duration again defined by the encryption quanta. By using a predefined encryption quanta, the

encryption pointers are simplified. By specifying the size of the encrypted segment, the size can be varied to achieve a more flexible encryption scheme, at the sacrifice of efficiency in the encryption pointers. Note that in the case of a predefined encryption quanta, multiple consecutive segments can be encrypted to achieve the effect of longer segments of encrypted content.

DRMs typically verify that the consumer has paid for viewing the content. Viewing may be granted for a period of time or on a viewing event. When a customer makes a payment, this act enables decryption of the content, often as a result of delivery of a decryption key to the customer to enable decryption. In order to enable two or more DRMs to work side-by-side, there should be a clear separation between the payment and key management operation and the content decryption. The media player should allow selection of either DRM. By use of selective encryption, most of the content can be sent in the clear with only certain critical or important content (needed to decompress the rest of the content) sent encrypted. The critical or important content is duplicated and one set of the content is encrypted under one DRM, while the other, is encrypted under the other DRM.

Movies and music delivered over the Internet can be packetized in UDP packets for delivery over IP networks. Once re-assembled in the PC, the file can be essentially flat. Both the video and audio can be large packetized elementary stream (PES) files.

In order to realize certain embodiments of the present invention, there should be agreement as to how a media player identifies content that is encrypted. In certain embodiments, the encryption quanta, if utilized, should be standardized, or there should be agreement on the least common denominator. Granularity of encryption should be standardized (e.g., can bits from different parts of a video and audio frame be collated for encryption? This is more complicated to signal unless the same bits are chosen over-and-over.). These matters, however, are more properly the subject of standardization negotiations

and are not important to the understanding of the concepts and principles governing the present invention.

The files described above can be created using any of a number of processes. Moreover, the file structure shown, although illustrated for audio/video content, can be readily adapted to audio only by omission of the video encryption pointers and video content. One process for creation of such files is depicted in **FIGURE 6** as process 600 starting at 604. At 608, a selection criterion is employed to select segments of content to be multiple selectively encrypted. The selection criterion used can be any of those described above, described in the above-referenced patent applications, described elsewhere or newly created without limitation. Once the segments of content are selected, they are duplicated as many times as there are DRM systems to be employed at 610. For example, in the digital content provider 104, one set of duplicate selected data is created.

The selected content is then multiple encrypted such that each of the duplicate sets of selected data is encrypted under the encryption scheme for each of the DRMs at 614. In the example of content provider 104, the selected segments of content are duplicated. One set of selected segments is encrypted under DRM A and the duplicate set is encrypted under DRM B. A set of encryption pointers is then created at 618 as offset values and possibly information that determines the size of the encrypted portions and the file can be saved in the content database 130 at this point until a customer wishes to acquire digital rights to the content. Alternatively, content can be stored in the clear (or encrypted) and the file for delivery to the customer can be created after purchase by the customer.

When a customer purchases rights to the content, a digital rights managed transaction is carried out at 626 in which the customer pays for certain rights. Such rights might include rights to view for a particular time period or number of viewings. Limitations can be imposed on copying, playback machine or other

attributes of the DRM during this transaction. When the transaction is complete, the file containing the purchased content is then retrieved from the content database and DRM data defining the purchased rights is appended at 630. The file is then downloaded or streamed to the customer at 634. The customer can then play back the content (either on computer 112 or another playback device) in a manner consistent with the DRM rights acquired in the transaction at 626.

Thus, a method of enabling use of multiple digital rights management scenarios (DRM), consistent with certain embodiments of the present invention involves examining unencrypted data representing digital content to identify at least segments of content for encryption; encrypting the identified segments of content using a first encryption method associated with a first DRM to produce first encrypted segments; encrypting the identified segments of content using a second encryption method associated with a second DRM to produce second encrypted segments; generating first pointers to the first encrypted content; generating second pointers to the second encrypted content; and replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, and inserting the first and second pointers to produce a partially encrypted dual DRM enabled file. When digital rights are purchased, DRM data enabling the rights are appended to the file and the file is sent to the customer.

A process such as that used by the customer in accordance with certain embodiments consistent with the present invention is illustrated as process 700 of **FIGURE 7** starting at 702 after which the customer acquires digital rights in content via a digital rights acquisition transaction at 706. The customer can then receive by download or streaming the multiple DRM file at 710. When the customer wishes to initiate playback at 714, the DRM data are read at 718, so that the software on the customer's computer or other playback device can determine if the digital rights acquired by the customer are valid (i.e., not expired or otherwise exhausted). If the software determines that the digital rights have

expired or been exhausted at 722, the playback is aborted at 726 and the process ends at 730.

If the customer's digital rights are verified at 722, the software reads the file's encryption pointers at 734 and begins reading the content at 738. If the content is encrypted at 742, it is decrypted at 746 according to the selected DRM scheme being used for playback (dependent upon the playback software and/or playback machine). If the content is unencrypted or decrypted, control passes to 750 where the content is played or buffered for play. If the end of the file has not been reached at 754, control passes back to 738 where a next segment of content is read. When the end of the file is reached at 754, the process stops at 730.

Thus, in accordance with certain embodiments consistent with the present invention, a method of using rights to digital content under one of a plurality of digital rights management scenarios (DRM), involves carrying out a transaction to acquire digital rights to the content; receiving digital content containing: segments of unencrypted content, first encrypted segments of content encrypted using a first encryption method associated with a first DRM, second encrypted segments of content encrypted using a second encryption method associated with a second DRM, first pointers to the first encrypted segments of content; second pointers to the second encrypted segments of content, and DRM data that enables digital rights under at least one of the first DRM and the second DRM; determining that valid digital rights are available from the DRM data; and decrypting one of the first and second encrypted segments to enable playing of the content.

The process 600 of **FIGURE 6** can be carried out on any suitable programmed general purpose processor operating as a multiple DRM encoder such as that depicted as computer 800 of **FIGURE 8**. Computer 800 has one or more central processor units (CPU) 810 with one or more associated buses 814 used to connect the central processor unit 810 to Random Access Memory 818

and Non-Volatile Memory 822 in a known manner. Output devices 826, such as a display and printer, are provided in order to display and/or print output for the use of the digital content provider as well as to provide a user interface such as a Graphical User Interface (GUI). Similarly, input devices such as keyboard, mouse and removable media readers 830 may be provided for the input of information by the operator. Computer 800 also incorporates internal and/or external attached disc or other mass storage 834 for storing large amounts of information including, but not limited to, the operating system, multiple DRM encryption methods, as well as the content (which is most likely stored on massive attached storage). The Computer system 800 also has an interface 838 for connection to the Internet to service customer requests for content. While depicted as a single computer, the digital content provider may utilize multiple linked computers to carry out the functions described herein.

The process 700 of **FIGURE 7** can be carried out on any suitable programmed general purpose processor operating as a decoder/decrypter and DRM validator such as that depicted as computer 900 of **FIGURE 9**. Computer 900 may be typical of personal computer devices and has a central processor unit (CPU) 910 with one or more associated buses 914 used to connect the central processor unit 910 to Random Access Memory 918 and Non-Volatile Memory 922 in a known manner. Output devices 926, such as a display adapter and display, are provided in order to display output for the use of the customer (possibly including playback of video content) as well as to provide a user interface such as a Graphical User Interface (GUI). An audio adapter and audio system 928 may also be attached for playback of audio or audio/video content. Similarly, input devices such as keyboard, mouse and removable media readers 930 may be provided for the input of information by the operator. Computer 900 also incorporates internal and/or external attached disc or other mass storage 934 for storing large amounts of information including, but not limited to, the operating system, DRM validation and decryption software, media player

software as well as the downloaded content. The Computer system 900 also has an interface 938 for connection to the Internet, e.g. to purchase content.

Thus, certain embodiments of the present invention provide for a digital content provider to readily supply content under multiple digital rights management schemes without need to fully encrypt the content for each potential DRM system. This permits a reduction in either storage capacity (for storage or multiple fully encrypted copies of content) or processing power (to encrypt on the fly) needed by the digital content provider. By use of embodiments of the present invention, the customer can be afforded a wide range of content without need to purchase or load multiple DRM systems and media players on his or her personal computer since multiple DRMs can be readily accommodated by the content provider at low cost.

Those skilled in the art will recognize that the present invention has been described in terms of exemplary embodiments based upon use of a programmed processor (e.g., computers 800 and 900). However, the invention should not be so limited, since the present invention could be implemented using hardware component equivalents such as special purpose hardware and/or dedicated processors which are equivalents to the invention as described and claimed. Similarly, general purpose computers, microprocessor based computers, micro-controllers, optical computers, analog computers, dedicated processors and/or dedicated hard wired logic may be used to construct alternative equivalent embodiments of the present invention. Moreover, although the present invention has been described in terms of a general purpose personal computer providing a playback mechanism, the playback can be carried on a dedicated machine without departing from the present invention.

Those skilled in the art will appreciate that the program steps and associated data used to implement the embodiments described above can be implemented using disc storage as well as other forms of storage such as for example Read Only Memory (ROM) devices, Random Access Memory (RAM)

devices; optical storage elements, magnetic storage elements, magneto-optical storage elements, flash memory, core memory and/or other equivalent storage technologies without departing from the present invention. Such alternative storage devices should be considered equivalents.

The present invention, as described in embodiments herein, is implemented using a programmed processor executing programming instructions that are broadly described above form that can be stored on any suitable electronic storage medium or transmitted over any suitable electronic communication medium or otherwise be present in any computer readable or propagation medium. However, those skilled in the art will appreciate that the processes described above can be implemented in any number of variations and in many suitable programming languages without departing from the present invention. For example, the order of certain operations carried out can often be varied, additional operations can be added or operations can be deleted without departing from the invention. Error trapping can be added and/or enhanced and variations can be made in user interface and information presentation without departing from the present invention. Such variations are contemplated and considered equivalent.

Software code and/or data embodying certain aspects of the present invention may be present in any computer readable medium, transmission medium, storage medium or propagation medium including, but not limited to, electronic storage devices such as those described above, as well as carrier waves, electronic signals, data structures (e.g., trees, linked lists, tables, packets, frames, etc.) optical signals, propagated signals, broadcast signals, transmission media (e.g., circuit connection, cable, twisted pair, fiber optic cables, waveguides, antennas, etc.) and other media that stores, carries or passes the code and/or data. Such media may either store the software code and/or data or serve to transport the code and/or data from one location to another. In the present exemplary embodiments, MPEG compliant packets, slices, tables and

other data structures are used, but this should not be considered limiting since other data structures can similarly be used without departing from the present invention.

While the invention has been described in conjunction with specific embodiments, it is evident that many alternatives, modifications, permutations and variations will become apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended that the present invention embrace all such alternatives, modifications and variations as fall within the scope of the appended claims.

What is claimed is:

1. A method of enabling use of multiple digital rights management scenarios (DRM), comprising:

examining unencrypted data representing digital content to identify at least segments of content for encryption;

encrypting the identified segments of content using a first encryption method associated with a first DRM to produce first encrypted segments;

encrypting the identified segments of content using a second encryption method associated with a second DRM to produce second encrypted segments;

generating first pointers to the first encrypted segments of content;

generating second pointers to the second encrypted segments of content; and

replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, and inserting the first and second pointers to produce a partially encrypted dual DRM enabled file.

2. The method according to claim 1, wherein the content comprises digitized audio.

3. The method according to claim 1, wherein the content comprises digitized video.

4. The method according to claim 1, further comprising appending data to enable digital rights under the first DRM to the file.

5. The method according to claim 1, further comprising appending data to enable digital rights under the second DRM to the file.

6. The method according to claim 1, wherein the first and second pointers comprise byte offsets identifying a starting location for encrypted segments of content.

7. The method according to claim 1, wherein the first and second encrypted segments of content have a duration defined by an encryption quanta.

8. The method according to claim 1, further comprising appending data to enable digital rights under at least one of the first DRM and the second DRM to the file; and transmitting the file to a customer.

9. A computer readable medium storing instructions which, when executed on a programmed processor, carry out the method of method of enabling use of multiple digital rights management scenarios according to claim 1.

10. An encoder that enables use of multiple digital rights management scenarios (DRM), comprising:

means for examining unencrypted data representing digital content to identify at least segments of content for encryption;

a first encrypter that encrypts the identified segments of content using a first encryption method associated with a first DRM to produce first encrypted segments;

a second encrypter that encrypts the identified segments of content using a second encryption method associated with a second DRM to produce second encrypted segments;

means for generating first pointers to the first encrypted segments of content;

means for generating second pointers to the second encrypted segments of content; and

means for replacing the identified segments of content with the first encrypted content and the second encrypted content in the digital content, and inserting the first and second pointers to produce a partially encrypted dual DRM enabled file.

11. The encoder according to claim 10, wherein the content comprises at least one of digitized audio and digitized video.

12. The encoder according to claim 10, further comprising means for appending data to enable digital rights under at least one of the first DRM and the second DRM to the file.

13. The encoder according to claim 10, wherein the first and second pointers comprise byte offsets identifying a starting location for encrypted segments of content.

14. The encoder according to claim 10, wherein the first and second encrypted segments of content have a duration defined by an encryption quanta.

15. The encoder according to claim 10, further comprising appending data to enable digital rights under at least one of the first DRM and the second DRM to the file; and transmitting the file to a customer.

16. The encoder according to claim 10, implemented in a programmed general purpose computer.

17. A method of using rights to digital content under one of a plurality of digital rights management scenarios (DRM), comprising:

carrying out a transaction to acquire digital rights to the content;

receiving digital content containing:

segments of unencrypted content,

first encrypted segments of content encrypted using a first encryption method associated with a first DRM,

second encrypted segments of content encrypted using a second encryption method associated with a second DRM,

first pointers to the first encrypted segments of content;

second pointers to the second encrypted segments of content, and

DRM data that enables digital rights under at least one of the first DRM and the second DRM;

determining that valid digital rights are available from the DRM data; and

decrypting one of the first and second encrypted segments to enable playing of the content.

18. The method according to claim 17, wherein the content comprises at least one of digitized audio and digitized video.

19. The method according to claim 17, wherein the first and second pointers comprise byte offsets identifying a starting location for encrypted segments of content.

20. The method according to claim 17, wherein the first and second encrypted segments of content have a duration defined by an encryption quanta.

21. A computer readable medium storing instructions which, when executed on a programmed processor, carry out the method of method of using rights to digital content according to claim 17.

22. A decoder that enables use rights to digital content under one of a plurality of digital rights management scenarios (DRM), comprising:

means for carrying out a transaction to acquire digital rights to the content;

means for receiving digital content containing:

segments of unencrypted content,

first encrypted segments of content encrypted using a first encryption method associated with a first DRM,

second encrypted segments of content encrypted using a second encryption method associated with a second DRM,

first pointers to the first encrypted segments of content;

second pointers to the second encrypted segments of content, and

DRM data that enables digital rights under at least one of the first DRM and the second DRM;

a DRM validator that determines that valid digital rights are available from the DRM data; and

a decrypter that decrypts one of the encrypted segments to enable playing the content.

23. The decrypter according to claim 22, wherein the content comprises at least one of digitized audio and digitized video.

24. The decrypter according to claim 22, wherein the first and second pointers comprise byte offsets identifying a starting location for encrypted segments of content.

25. The decrypter according to claim 22, wherein the first and second encrypted segments of content have a duration defined by an encryption quanta.

26. The decrypter according to claim 22, implemented in a programmed general purpose computer.

27. A selectively encrypted digital content signal that enables use of multiple digital rights management scenarios (DRM) embodied in a carrier wave, comprising:

segments of unencrypted content;

first encrypted segments of content encrypted using a first encryption method associated with a first DRM;

second encrypted segments of content encrypted using a second encryption method associated with a second DRM;

a first segment of code comprising first pointers to the first encrypted segments of content;

a second segment of code comprising second pointers to the second encrypted segments of content; and

a segment of DRM data that enables digital rights under at least one of the first DRM and the second DRM.

28. The carrier wave according to claim 27, wherein the content comprises at least one of digitized audio and digitized video.

29. The carrier wave according to claim 27, wherein the first and second pointers comprise byte offsets identifying a starting location for encrypted segments of content.

30. The carrier wave according to claim 27, wherein the first and second encrypted segments of content have a duration defined by an encryption quanta.

31. A selectively encrypted digital content signal that enables use of multiple digital rights management scenarios (DRM) embodied in a computer readable medium, comprising:

segments of unencrypted content;

first encrypted segments of content encrypted using a first encryption method associated with a first DRM;

second encrypted segments of content encrypted using a second encryption method associated with a second DRM;

a first segment of code comprising first pointers to the first encrypted segments of content;

a second segment of code comprising second pointers to the second encrypted segments of content; and

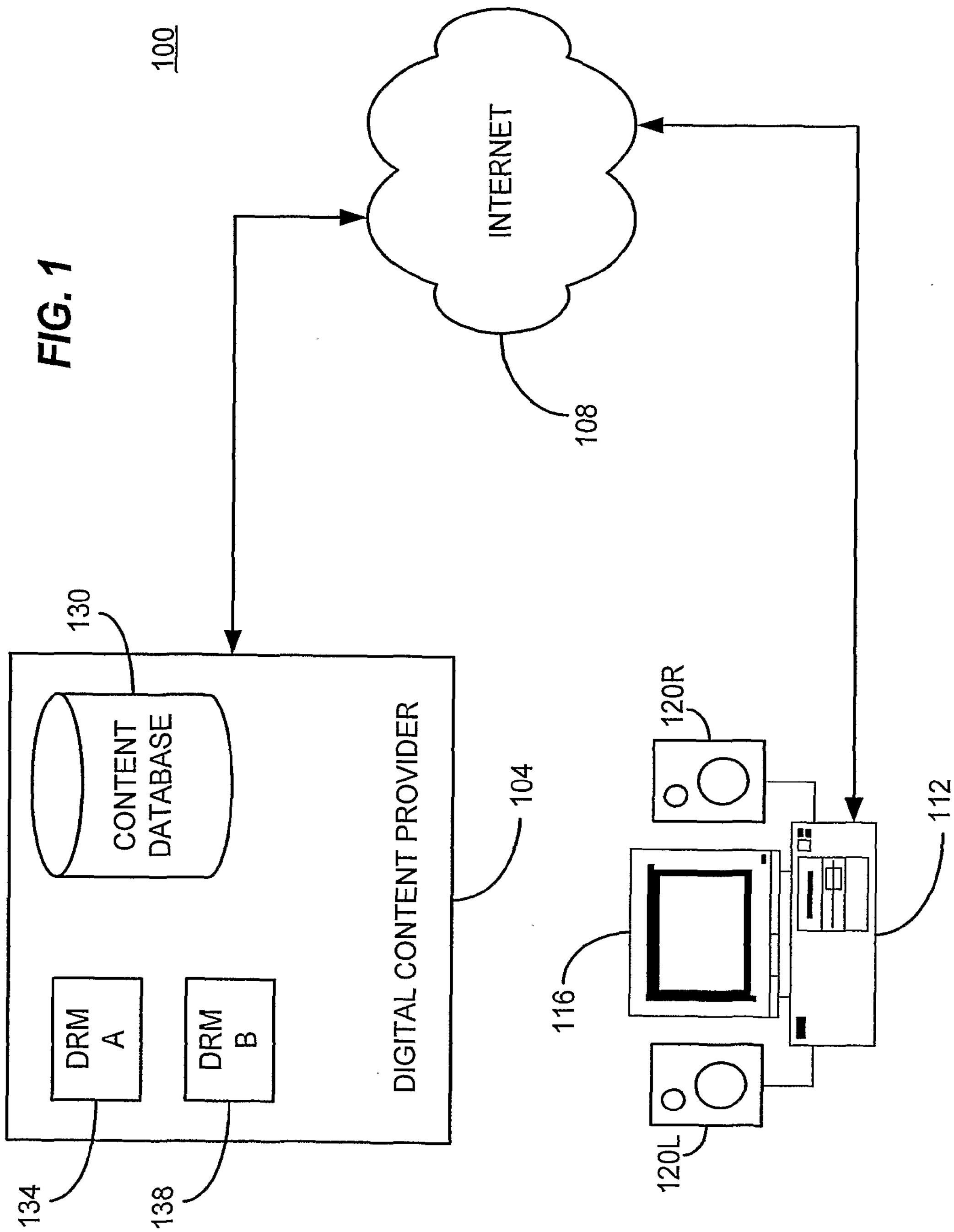
a segment of DRM data that enables digital rights under at least one of the first DRM and the second DRM.

32. The computer readable medium according to claim 31, wherein the content comprises at least one of digitized audio and digitized video.

33. The computer readable medium according to claim 31, wherein the first and second pointers comprise byte offsets identifying a starting location for encrypted segments of content.

34. The computer readable medium according to claim 31, wherein the first and second encrypted segments of content have a duration defined by an encryption quanta.

FIG. 1


100
INTERNET
108
CONTENT
DATABASE
130
DRM
A
DRM
B
DIGITAL CONTENT PROVIDER
104
134
138
120R
120L
116
112

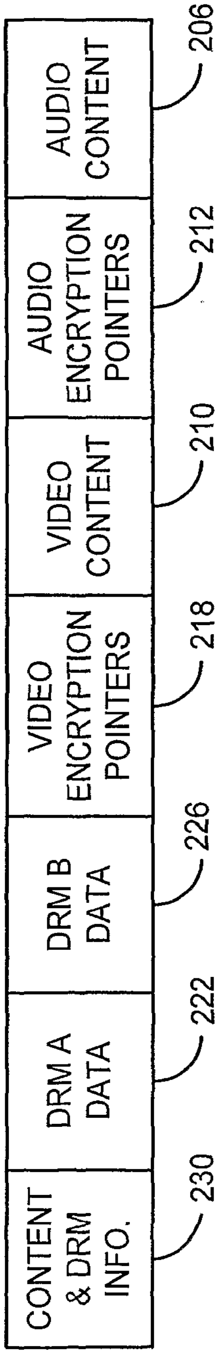


FIG. 2

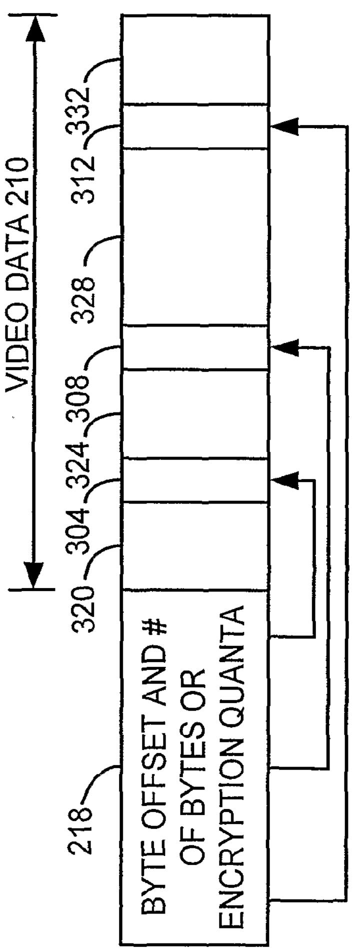


FIG. 3

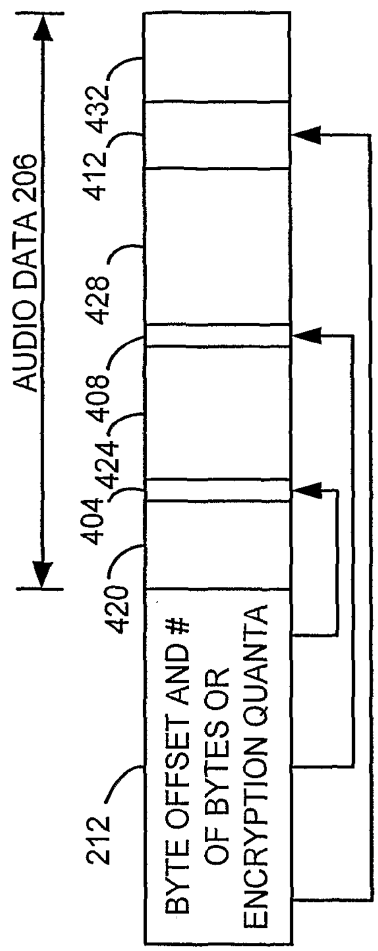


FIG. 4

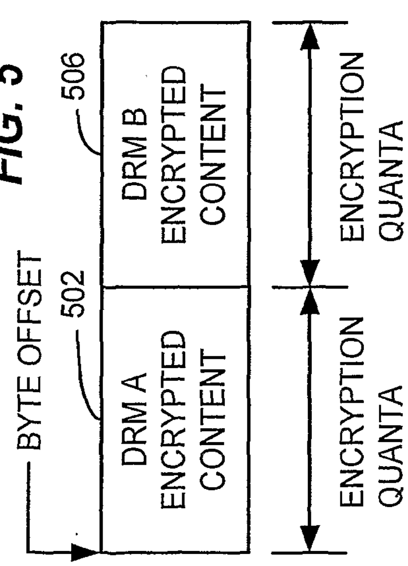


FIG. 5

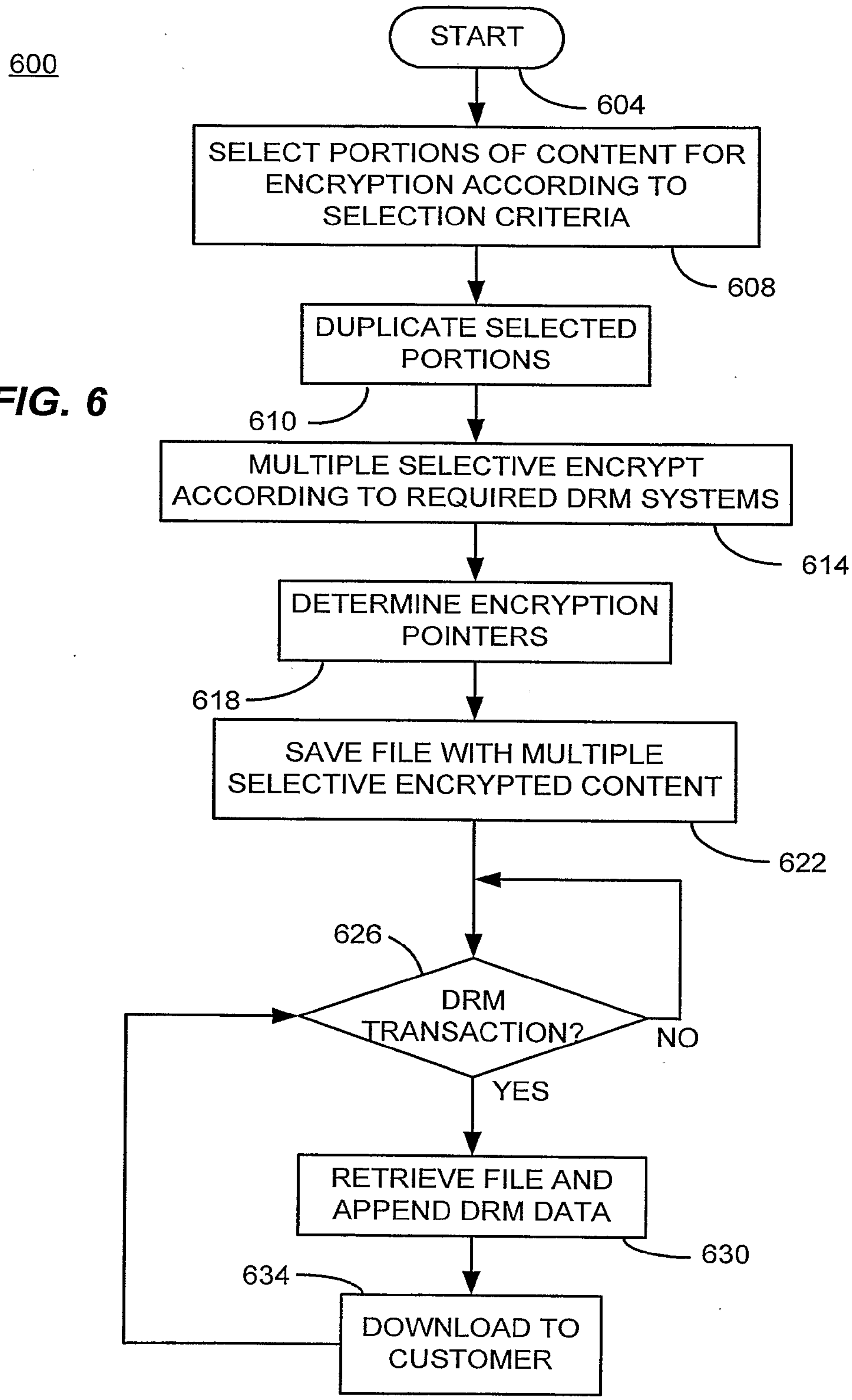

600
START
604
SELECT PORTIONS OF CONTENT FOR ENCRYPTION ACCORDING TO SELECTION CRITERIA
608
DUPLICATE SELECTED PORTIONS
610
MULTIPLE SELECTIVE ENCRYPT ACCORDING TO REQUIRED DRM SYSTEMS
614
DETERMINE ENCRYPTION POINTERS
618
SAVE FILE WITH MULTIPLE SELECTIVE ENCRYPTED CONTENT
622
626
DRM TRANSACTION?
NO
YES
RETRIEVE FILE AND APPEND DRM DATA
630
634
DOWNLOAD TO CUSTOMER

FIG. 6

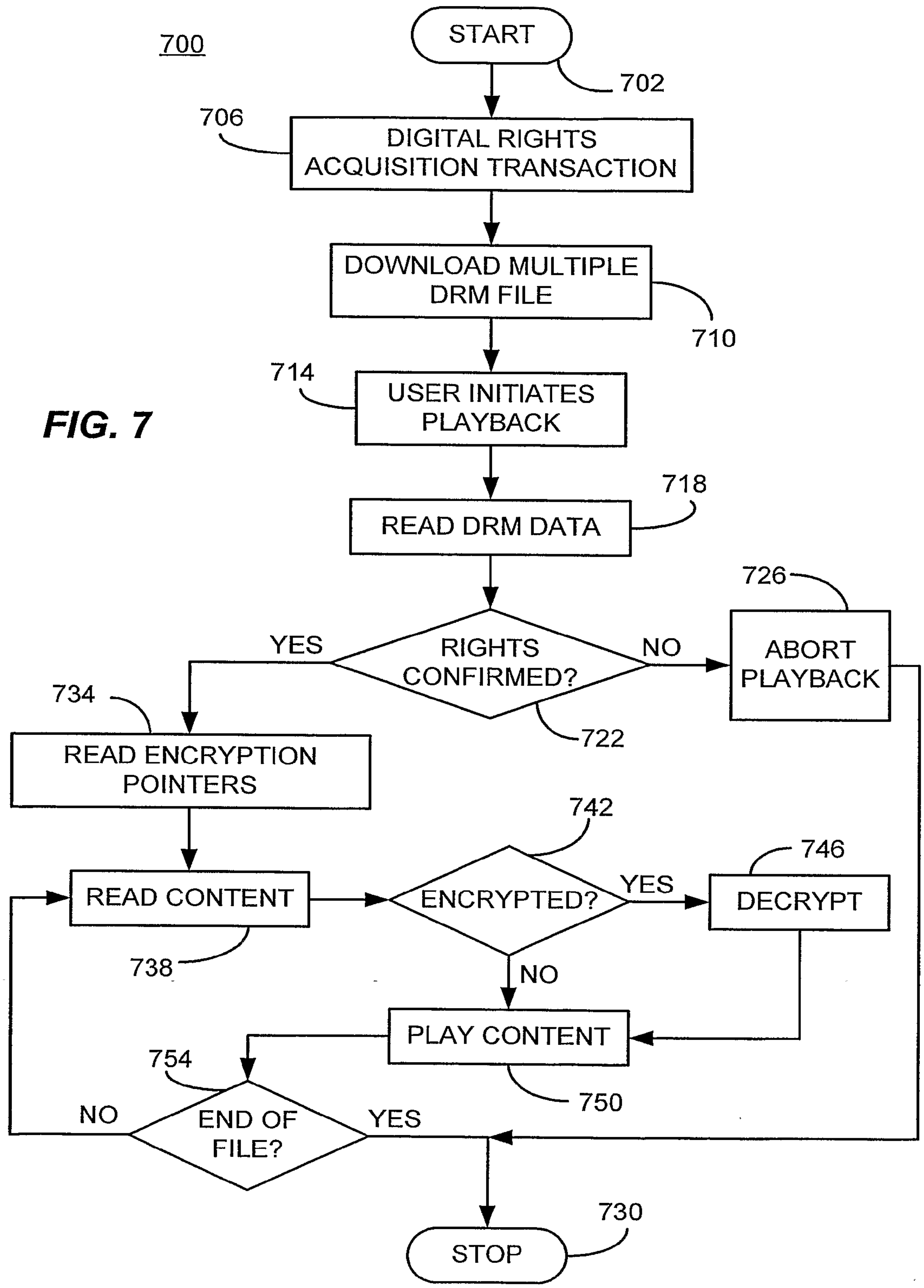

700
START
702
706
DIGITAL RIGHTS ACQUISITION TRANSACTION
DOWNLOAD MULTIPLE DRM FILE
710
714
USER INITIATES PLAYBACK
718
READ DRM DATA
726
YES
RIGHTS CONFIRMED?
NO
ABORT PLAYBACK
734
722
READ ENCRYPTION POINTERS
742
746
READ CONTENT
ENCRYPTED?
YES
DECRYPT
738
NO
PLAY CONTENT
754
750
NO
END OF FILE?
YES
730
STOP

FIG. 7

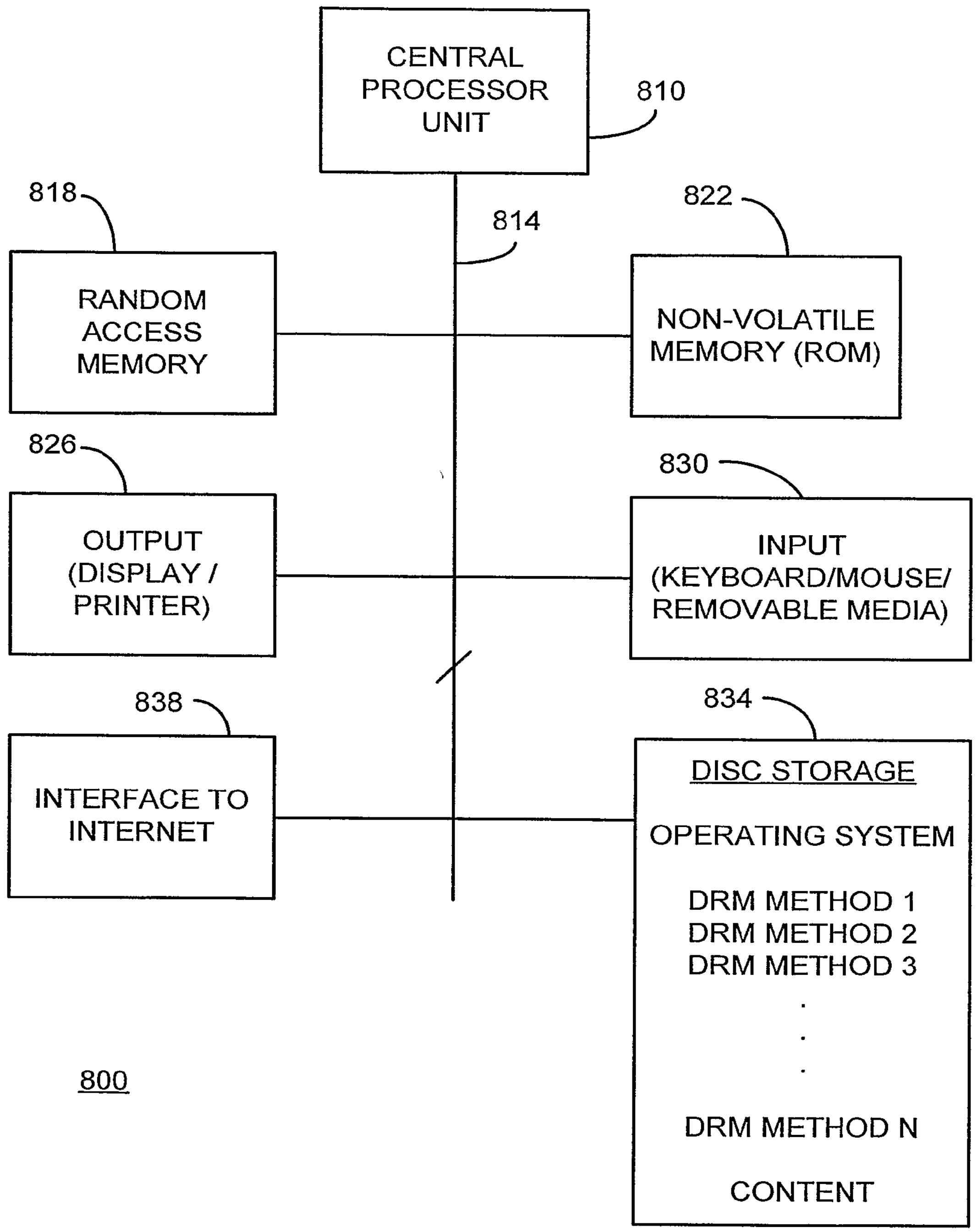

CENTRAL PROCESSOR UNIT
810
818
814
822
RANDOM ACCESS MEMORY
NON-VOLATILE MEMORY (ROM)
826
830
OUTPUT (DISPLAY / PRINTER)
INPUT (KEYBOARD/MOUSE/ REMOVABLE MEDIA)
838
834
INTERFACE TO INTERNET
DISC STORAGE
OPERATING SYSTEM
DRM METHOD 1
DRM METHOD 2
DRM METHOD 3
DRM METHOD N
CONTENT
800

FIG. 8

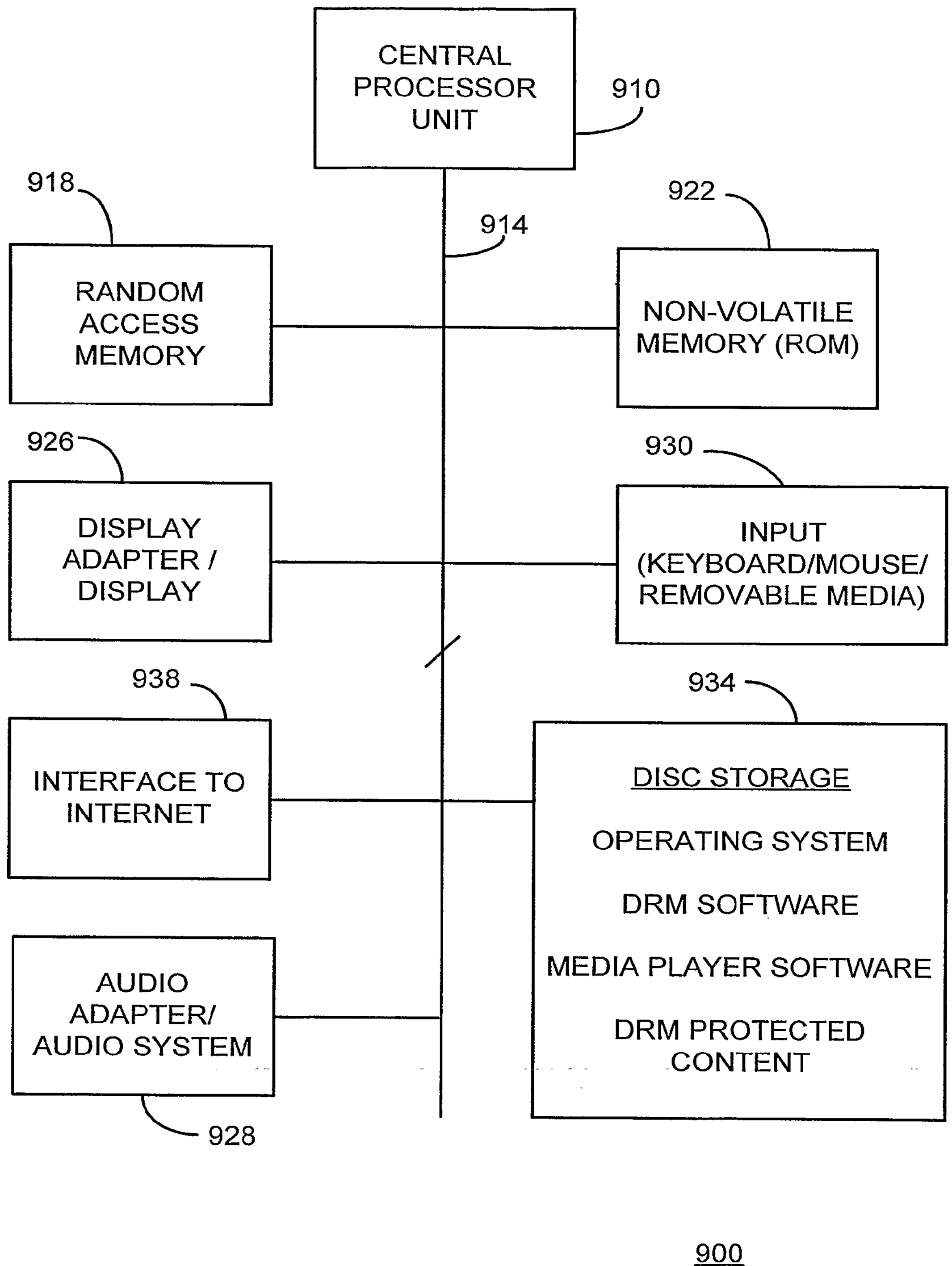

CENTRAL PROCESSOR UNIT
910
914
918
RANDOM ACCESS MEMORY
922
NON-VOLATILE MEMORY (ROM)
926
DISPLAY ADAPTER / DISPLAY
930
INPUT (KEYBOARD/MOUSE/ REMOVABLE MEDIA)
938
INTERFACE TO INTERNET
934
DISC STORAGE
OPERATING SYSTEM
DRM SOFTWARE
MEDIA PLAYER SOFTWARE
DRM PROTECTED CONTENT
AUDIO ADAPTER/ AUDIO SYSTEM
928
900

FIG. 9